Two New Zero-Dimensional Qubit Codes from Bordered Metacirculant Construction

Padmapani Seneviratne\textsuperscript{a}, Martianus Frederic Ezerman\textsuperscript{a,b}

\textsuperscript{a}Department of Mathematics, Texas A&M University-Commerce, 2600 South Neal Street, Commerce TX 75428, U.S.A.

\textsuperscript{b}School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371.

Abstract

We construct qubit stabilizer codes with parameters \([81,0,20]_K\) and \([94,0,22]_K\) for the first time. We use symplectic self-dual additive codes over \(F_4\) built by modifying the adjacency matrices of suitable metacirculant graphs found by a randomized search procedure.

Key words: additive codes, graph codes, quantum codes, metacirculant graph, self-dual codes

1. Introduction

Let \(\omega\) be a root of \(x^2 + x + 1 \in F_2[x]\). The finite field of 4 element is \(F_4 := \{0, 1, \omega, \omega^2 = \bar{\omega}\}\). A code \(C\) of length \(n\) over \(F_4\) is additive if the sum of any two, not necessarily distinct, codewords \(c, w \in C\) is again a codeword in \(C\). The weight of a vector in \(F_4^n\) is the number of its nonzero entries. The distance of vectors \(a, b \in F_4^n\) is the number of positions where their respective entries differ. The minimum distance of an additive code \(C\) is the smallest weight \(d\) among the weights of its nonzero codewords. The code is Type II if each of its codewords has an even weight. Otherwise, \(C\) is Type I. If \(|C| = 2^k\), then it has the parameters \((n, 2^k, d)_4\).

The trace Hermitian inner product of \(a, b \in F_4^n\) is

\[
\mathbf{a} \ast \mathbf{b} = \sum_{j=1}^{n} (a_j b_j^2 + \bar{a}_j^2 b_j).
\]

The code \(C^* = \{w \in F_4^n : \mathbf{w} \ast \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C\}\) is the symplectic dual of \(C\) and \(C\) is self-dual if \(C = C^*\). A self-dual additive code \(C\) over \(F_4\) directly leads to a quantum bit (qubit) stabilizer code \(Q := Q(C)\) with parameters \([n, 0, d]_2\). This link is so well-established that we simply refer the readers to the exposition of Calderbank, Rains, Shor, and Sloane in \textit{[3]} for the details. The zero dimensional qubit code \(Q\) represents a highly entangled single quantum state, useful when high entanglement and error-correction rate are simultaneously required.
Let $G$ be a simple undirected graph with $n$ vertices and adjacency matrix $\Gamma := \Gamma(G)$. A graph code on $G$ is an $(n, 2^n, d)_4$ additive code $C := C(G)$ whose codewords are the $\mathbb{F}_2$-linear combinations of the rows of $\Gamma + \omega I_n$. Any graph code is clearly self-dual. Various versions and proofs of the following main result, first discussed by Schlingemann in [11], are nicely presented by Danielsen and Parker in [4, Section 3]. Every graph represents a self-dual additive code over $\mathbb{F}_4$ and every self-dual additive code over $\mathbb{F}_4$ can be represented by a graph. Thus, to construct $[n, 0, d]_2$ stabilizer codes, it suffices to find graph codes with minimum distance $d$. Two graph codes are equivalent if their corresponding graphs are isomorphic [4, Thm. 6].

A complete classification of all self-dual additive codes over $\mathbb{F}_4$ for $n \leq 12$ was done in [4]. Follow-up works, covering $n \leq 50$, were done by Gulliver and Kim in [8], by Varbanov in [12], by Grassl and Harada in [7], and by Saito in [10]. Their efforts were limited mostly to graphs whose adjacency matrices are circulant or bordered circulant. Excellent has been observed to come from strongly regular graphs with large symmetry groups. As $n$ grows, the challenge to search for, much less classify, codes with optimal $d$ escalates since computing the exact minimum distance is hard [13].

In [9] we restricted the graphs to the metacirculant family. In the present work, the new $[81, 0, 20]_2$ and $[94, 0, 24]_2$ codes come from bordered metacirculant graphs. For $n \in \{29, 37\}$ we obtain bordered metacirculant graph codes with strictly better minimum distances than the best bordered circulant ones.

2. Bordered Metacirculant Graphs

Definition 1. ([1]) Let $m, \ell \in \mathbb{N}$ be fixed and $\alpha \in \mathbb{Z}_\ell$ be a unit. Let $S_0, S_1, \ldots, S_{\lfloor m/2 \rfloor} \subseteq \mathbb{Z}_\ell$ satisfy the four properties

1. $S_0 = -S_0$,
2. $0 \notin S_0$,
3. $\alpha^m S_k = S_k$ for $1 \leq k \leq \lfloor m/2 \rfloor$,
4. if $m$ is even, then $\alpha^{m/2} S_{m/2} = -S_{m/2}$.

The metacirculant graph $G := G(m, \ell, \alpha, S_0, S_1, \ldots, S_{\lfloor m/2 \rfloor})$ has as its vertex set $V(G) := \mathbb{Z}_m \times \mathbb{Z}_\ell$ of size $n = m \cdot \ell$. Let $V_0, V_1, \ldots, V_{m-1}$, where $V_j = \{(i, j) : 0 \leq j < \ell\}$, be a partition of $V(G)$. Let $1 \leq k \leq \lfloor m/2 \rfloor$. Vertices $(i, j)$ and $(i+k, h)$ are adjacent if and only if $(h-j) \in \alpha^k S_k$. The adjacency matrix $\Gamma := \Gamma(G)$ of a metacirculant graph $G$ is a metacirculant matrix. A bordered metacirculant matrix

$$\Gamma = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & \ldots & \Gamma \\ \vdots & \ddots & \vdots \\ 1 & & \end{bmatrix},$$

is the adjacency matrix of the graph $\overline{G}$, obtained from $G$ by adding a new vertex $v_\infty$ and joining $v_\infty$ to each vertex of $G$. 

2
Thus follows the desired conclusion.

**Proof.**

An additive graph code $C$ from a circulant graph code was recorded in [8, Table II]. Its corresponding $[29,0,11]_4$ code is unique, up to equivalence [12].

**Example 1.** The unique $[[6,0,4]]_2$ code is from the $(6,2^6,4)_4$ hexacode, which can be derived from the metacirculant graph $G_6 := G(2,3,1,\{1,2\},\{0\})$. Figure 1 labels vertices in $V_0 = \{(0,0),(0,1),(0,2)\}$ and $V_1 = \{(1,0),(1,1),(1,2)\}$ as 1,2,…,6. The adjacency matrix $\Gamma_6$ of $G_6$ and the generator matrix $\Gamma_6 + \omega I_7$ of the self-dual $(7,2^7,3)_4$ code are, respectively,

$$
\begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 \\
\end{bmatrix}
\quad\begin{bmatrix}
\omega & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & \omega & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & \omega & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & \omega & 0 & 0 & 1 & 0 & 1 & \omega \\
1 & 1 & 0 & 0 & \omega & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & \omega & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & \omega \\
\end{bmatrix}
$$

The highest $d$ of an additive self-dual $(29,2^{29},d)_4$ codes from the bordered circulant graph construction is $d = 9$, as shown in [10]. Using the bordered metacirculant graph construction, we obtain a self-dual $(29,2^{29},10)_4$ code $C_{29}$. The strict improvement in $d$ in Proposition 1 does not carry over to the quantum setup. The code $C_{29}$ gives a $[[29,0,10]]_2$ stabilizer code. A better $[[29,0,11]]_2$ code from a circulant graph code was recorded in [8, Table II]. Its corresponding $(29,2^{29},11)_4$ circulant code is unique, up to equivalence [12].

**Proposition 1.** The bordered metacirculant graph $G_{28}$ with

$$
G_{28} := G(2,14,13,\{5,6,8,9\},\{0,1,3,6,7,9,11\})
$$

in Table 1 generates a self-dual $(29,2^{29},10)_4$ code $C_{29}$.

**Theorem 2.** Let $C$ be an additive symplectic self-dual code over $\mathbb{F}_4$ generated by a bordered metacirculant $\Gamma(m,\ell,\alpha,S_0,S_1,\ldots,S_{[m/2]})$. Let $\Delta_S := |S_0| + 1$ if $m$ is odd and $\Delta_S := |S_0| + |S_{[m/2]}| + 1$ if $m$ is even. Then $C$ is Type II if and only if both $\Delta_S$ and $n = m \cdot \ell$ are odd.

**Proof.** An additive graph code $C(G)$ is Type II if and only if all vertices of $G$ are of odd degree [4]. In the bordered metacirculant $\Gamma(m,\ell,\alpha,S_0,S_1,\ldots,S_{[m/2]})$, $\deg(v_o) = m \cdot \ell$ and

$$
\deg(v) = \begin{cases}
|S_0| + |S_1| + 1 & \text{when } m = 2, \\
|S_0| + |S_{[m/2]}| + 2 \left(\sum_{i=1}^{[m/2]-1} |S_i|\right) + 1 & \text{for even } m \geq 4, \\
|S_0| + 2 \left(\sum_{i=1}^{[m/2]} |S_i|\right) + 1 & \text{for odd } m \geq 3.
\end{cases}
$$

Thus follows the desired conclusion. \qed
There are at least two inequivalent self-dual additive Proposition 3. Using the bordered metacirculant construction, we found two inequivalent codes. The complete edge sets of the corresponding metacirculant graphs are given in Table 2.

**Proposition 3.** There are at least two inequivalent self-dual additive \((37, 2^{37}, 11)_4\) codes, built respectively from the graphs

\[
\overline{G}_{36,1} := \overline{G}(2, 18, 17, \{1, 3, 9, 15, 17\}, \{2, 6, 8, 11, 15, 16\}) \quad \text{and} \\
\overline{G}_{36,2} := \overline{G}(2, 18, 17, \{1, 2, 3, 5, 13, 15, 16, 17\}, \{0, 1, 2, 3, 5, 8, 9, 11, 12, 13, 15\}). \quad (3) (4)
\]

The codes have, respectively, 252 and 270 codewords of weight 11. The corresponding \([37, 0, 11]_2\) code has the best-known parameters \([5]\).

3. Two new qubit codes

We present two new codes found via a randomized search for bordered metacirculant graphs. Calculating the minimum distances of \(Q_{81, 1}\) and \(Q_{94}\) in Magma \([2]\) took 6 and 27 days. Secondary constructions often derive qubit codes that perform better than the current best-known. They are explained, for example, in \([3\), Theorem 6\] and \([6\), Section 4\]. These propagation rules are routinely performed on all new submissions to the online table and improved codes, if found, are then put on record. We omit the derivation of possibly new codes by secondary constructions.

**Proposition 4.** For \(k \in \{1, 2, 3\}\), each \(Q_{80,k}\) with \(G_{80,k}\) given respectively by

\[
G(8, 10, 7, \{1, 4, 6, 9\}, \{0, 1, 2, 3, 6, 7, 8\}, \{0, 2, 3, 4, 8, 9\}, \{0, 6\}, \{0, 1, 2, 4, 6, 8, 9\}), \quad (5) \\
G(8, 10, 3, \{4, 5, 6\}, \{0, 1, 2, 4, 5, 7, 9\}, \{0, 1, 5, 8, 9\}, \{0, 2, 3, 7\}, \{1, 2, 3, 4, 5, 6, 7, 8, 9\}), \quad (6) \\
G(10, 8, 5, \{2, 3, 5, 6\}, \{3\}, \{2, 4, 6, 7\}, \{5, 6\}, \{0, 1, 2, 3, 4, 6\}, \{0, 2, 5, 6, 7\}), \quad (7)
\]

generates a new \((81, 2^{81}, 20)_4\) Type I additive self-dual code. The corresponding \([81, 0, 20]_2\) code \(Q_{81,k}\) improves on the \([81, 0, 19]_2\) code in \([5\). Table 3 lists the edges of \(G_{80,1}\).

**Proposition 5.** The bordered metacirculant graph \(G_{93}\) with

\[
G_{93} := G(3, 31, 1, \{10, 12, 13, 15, 16, 18, 19, 21\}, \{4, 6, 7, 9, 12, 14, 15, 18, 19, 21\}) \quad (8)
\]
Table 2: The 198 and 342 respective edges of $G_{18.1}$ and $G_{18.2}$ as $(i, \{ j \in J \})$. For $0 \leq t < 18$, vertices $(0,t)$ are 1 to 18 while $(1,t)$ are 19 to 36.

\[
\begin{align*}
&\{1, (3,6,7,14,18,19,24,31,32,33,34,35)\}, \{2, (4,5,7,8,15,20,21,25,32,33,36)\}, \\
&\{3, (5,8,9,16,20,21,26,33,34,36)\}, \{4, (6,7,9,10,17,22,23,27,34,35)\}, \\
&\{5, (7,10,11,18,22,23,28,35,36)\}, \{6, (8,9,11,12,19,24,25,29,36)\}, \\
&\{7, (9,12,13,20,24,25,30)\}, \{8, (10,11,13,14,21,26,27,31)\}, \{9, (11,14,15,22,26,27,32)\}, \\
&\{10, (12,13,15,16,23,28,29,33)\}, \{11, (13,16,17,24,28,29,34)\}, \\
&\{12, (14,15,17,18,25,30,31,35)\}, \{13, (15,18,19,26,30,31,36)\}, \\
&\{14, (16,17,19,20,27,32,33)\}, \{15, (17,20,21,28,32,33)\}, \{16, (18,19,21,22,29,34,35)\}, \\
&\{17, (19,22,23,30,34,35)\}, \{18, (20,21,23,24,31,36)\}, \{19, (21,24,25,32,36)\}, \\
&\{20, (22,23,25,26,33)\}, \{21, (23,26,27,34)\}, \{22, (24,25,27,28,35)\}, \\
&\{23, (25,28,29,36)\}, \{24, (26,27,29,30)\}, \{25, (27,30,31)\}, \{26, (28,31,32)\}, \\
&\{27, (29,32,33)\}, \{28, (30,31,33,34)\}, \{29, (31,34,35)\}, \{30, (32,33,35,36)\}, \\
&\{31, (33,36)\}, \{32, (34,35)\}, \{33, (35)\}, \{34, (36)\}.
\end{align*}
\]
Table 3: The 1640 edges of $G_{10}$ as $(i, \{j \in I\})$, where $i, j$ are indices of the adjacent vertices. Vertices are partitioned into $V_0, V_1, \ldots, V_{10}$ with the 10 vertices in $V_i$ having the coordinates $z_i, z_i + 1, \ldots, z_i + 9$ for $0 \leq k < 8$ and $z_i + 10 + k$.

<table>
<thead>
<tr>
<th>i, j</th>
<th>0, 8</th>
<th>1, 9</th>
<th>2, 7</th>
<th>3, 6</th>
<th>4, 5</th>
<th>4, 5</th>
<th>4, 5</th>
<th>4, 5</th>
<th>4, 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2</td>
<td>(45, 47)</td>
<td>(48, 50)</td>
<td>(51, 53)</td>
<td>(54, 56)</td>
<td>(57, 59)</td>
<td>(60, 62)</td>
<td>(63, 65)</td>
<td>(66, 68)</td>
<td>(69, 71)</td>
</tr>
<tr>
<td>2, 3</td>
<td>(46, 48)</td>
<td>(51, 53)</td>
<td>(54, 56)</td>
<td>(57, 59)</td>
<td>(60, 62)</td>
<td>(63, 65)</td>
<td>(66, 68)</td>
<td>(69, 71)</td>
<td>(72, 74)</td>
</tr>
<tr>
<td>3, 4</td>
<td>(47, 49)</td>
<td>(52, 54)</td>
<td>(55, 57)</td>
<td>(58, 60)</td>
<td>(61, 63)</td>
<td>(64, 66)</td>
<td>(67, 69)</td>
<td>(70, 72)</td>
<td>(73, 75)</td>
</tr>
<tr>
<td>4, 5</td>
<td>(48, 50)</td>
<td>(53, 55)</td>
<td>(56, 58)</td>
<td>(59, 61)</td>
<td>(62, 64)</td>
<td>(65, 67)</td>
<td>(68, 70)</td>
<td>(71, 73)</td>
<td>(74, 76)</td>
</tr>
<tr>
<td>5, 6</td>
<td>(49, 51)</td>
<td>(54, 56)</td>
<td>(57, 59)</td>
<td>(60, 62)</td>
<td>(63, 65)</td>
<td>(66, 68)</td>
<td>(69, 71)</td>
<td>(72, 74)</td>
<td>(75, 77)</td>
</tr>
<tr>
<td>6, 7</td>
<td>(50, 52)</td>
<td>(55, 57)</td>
<td>(58, 60)</td>
<td>(61, 63)</td>
<td>(64, 66)</td>
<td>(67, 69)</td>
<td>(70, 72)</td>
<td>(73, 75)</td>
<td>(76, 78)</td>
</tr>
<tr>
<td>7, 8</td>
<td>(51, 53)</td>
<td>(56, 58)</td>
<td>(59, 61)</td>
<td>(62, 64)</td>
<td>(65, 67)</td>
<td>(68, 70)</td>
<td>(71, 73)</td>
<td>(74, 76)</td>
<td>(77, 79)</td>
</tr>
<tr>
<td>8, 9</td>
<td>(52, 54)</td>
<td>(57, 59)</td>
<td>(60, 62)</td>
<td>(63, 65)</td>
<td>(66, 68)</td>
<td>(69, 71)</td>
<td>(72, 74)</td>
<td>(75, 77)</td>
<td>(78, 80)</td>
</tr>
<tr>
<td>9, 10</td>
<td>(53, 55)</td>
<td>(58, 60)</td>
<td>(61, 63)</td>
<td>(64, 66)</td>
<td>(67, 69)</td>
<td>(70, 72)</td>
<td>(73, 75)</td>
<td>(74, 76)</td>
<td>(77, 79)</td>
</tr>
</tbody>
</table>

| 10, 11 | (54, 56) | (59, 61) | (62, 64) | (65, 67) | (68, 70) | (71, 73) | (74, 76) | (75, 77) | (78, 80) |
| 11, 12 | (55, 57) | (60, 62) | (63, 65) | (66, 68) | (69, 71) | (72, 74) | (75, 77) | (76, 78) | (79, 81) |
| 12, 13 | (56, 58) | (61, 63) | (64, 66) | (67, 69) | (70, 72) | (73, 75) | (74, 76) | (75, 77) | (78, 80) |
| 13, 14 | (57, 59) | (62, 64) | (65, 67) | (68, 70) | (71, 73) | (74, 76) | (75, 77) | (76, 78) | (79, 81) |
| 14, 15 | (58, 60) | (63, 65) | (66, 68) | (69, 71) | (72, 74) | (75, 77) | (76, 78) | (77, 79) | (80, 82) |
| 15, 16 | (59, 61) | (64, 66) | (67, 69) | (70, 72) | (73, 75) | (74, 76) | (75, 77) | (76, 78) | (79, 81) |
| 16, 17 | (60, 62) | (65, 67) | (68, 70) | (71, 73) | (74, 76) | (75, 77) | (76, 78) | (77, 79) | (80, 82) |
| 17, 18 | (61, 63) | (66, 68) | (69, 71) | (72, 74) | (75, 77) | (76, 78) | (77, 79) | (78, 80) | (81, 83) |
| 18, 19 | (62, 64) | (67, 69) | (70, 72) | (73, 75) | (74, 76) | (75, 77) | (76, 78) | (77, 79) | (80, 82) |
| 19, 20 | (63, 65) | (68, 68) | (69, 71) | (72, 74) | (75, 77) | (76, 78) | (77, 79) | (78, 80) | (81, 83) |
| 20, 21 | (64, 66) | (69, 71) | (72, 74) | (75, 77) | (76, 78) | (77, 79) | (78, 80) | (79, 81) | (82, 84) |
| 21, 22 | (65, 67) | (70, 72) | (73, 75) | (74, 76) | (75, 77) | (76, 78) | (77, 79) | (78, 80) | (81, 83) |
| 22, 23 | (66, 68) | (71, 73) | (72, 74) | (73, 75) | (74, 76) | (75, 77) | (76, 78) | (77, 79) | (80, 82) |
| 23, 24 | (67, 69) | (72, 74) | (73, 75) | (74, 76) | (75, 77) | (76, 78) | (77, 79) | (78, 80) | (81, 83) |
| 24, 25 | (68, 70) | (73, 75) | (74, 76) | (75, 77) | (76, 78) | (77, 79) | (78, 80) | (79, 81) | (82, 84) |
| 25, 26 | (69, 71) | (74, 76) | (75, 77) | (76, 78) | (77, 79) | (78, 80) | (79, 81) | (80, 82) | (83, 85) |
| 26, 27 | (70, 72) | (75, 77) | (76, 78) | (77, 79) | (78, 80) | (79, 81) | (80, 82) | (81, 83) | (84, 86) |
generates a new \( (94, 2^{94}, 22)_4 \) Type II additive self-dual code \( C_{94} \). The corresponding \( [94, 0, 22]_2 \) code \( Q_{94} \) improves the minimum distance of the \( [94, 0, 20]_2 \) code in \([5]\) by 2. The vertex set of \( G_{93} \) are partitioned into \( V_0, V_1, V_2 \), each containing the respective 31 vertices in \( \{(k,t) : k \in \{0, 1, 2\}, 0 \leq t < 31\} \). Table \( 4 \) presents the edge set of \( G_{93} \) based on the partition.

Table \( 5 \) gives the properties of the graphs. All have diameter 2 and girth 3, except for \( G_{36, 1} \) whose diameter is 3. Listed are the minimum distance \( d_{\text{min}}(C) \) of \( C := C(G) \), the valency \( v(G) \), the maximum clique size \( \gamma(G) \), and the size \( |\text{Aut}(G)| \) of the automorphism group.

Acknowledgements

Nanyang Technological University Grant Number 04INS000047C230GRT01 supports the research carried out by M. F. Ezerman.

References

Table 4: The 1302 Edges of G0. Vertices 1 to 31 relabel those in V0. Vertices 32 to 63 stand in place of those in V1. Vertices 64 to 93 rename the ones in V1. The tuple (r,s) indicates that i is in Vr and j is in Vs for r ≠ s. The presentation allows us to observe if an edge connects two vertices within the same Vr or two vertices in Vr and j is in Vs with r ≠ s.

Graph d_{min}(G) γ(G) ω(G) |Aut(G)| |Aut(G)|
---|---|---|---|---|---
G28 |11|11|4|28|G80,120|41|8|80|
G36,1 |11|14|3|6|G80,220|44|7|80|
G36,2 |11|19|5|36|G80,320|35|9|80|
G93 |22|28|4|186|G93|22|28|4|186|

Table 5: Properties of the Graphs

| Graph | d_{min}(G) | γ(G) | ω(G) | |Aut(G)| |Aut(G)| |
|---|---|---|---|---|---|---|---|
|G28 |10|11|4|28|G80,120|41|8|80|
|G36,1 |11|14|3|6|G80,220|44|7|80|
|G36,2 |11|19|5|36|G80,320|35|9|80|
|G93 |22|28|4|186|G93|22|28|4|186|

8